IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Identifying and Mitigating Network Vulnerabilities Using Ethical Hacking Methodologies

[1]Y N Priya, [2]Dr. V S Krushnasamy

[1]Student, [2]Associate Professor
Department of Electronics and Instrumentation Engineering
Dayananda Sagar College of Engineering, Bangalore, India

Abstract : Unauthorized access, control, or manipulation of computer systems and networks is referred to as "system hacking." This essay examines the methods and resources frequently employed in system hacking, such as keylogging, privilege escalation, password cracking, and backdoor installation. The focus is on comprehending how attackers take use of flaws in network setups, user behaviour, and operating systems. The phases of system hacking—reconnaissance, access acquisition, access maintenance, and trace removal—are thoroughly examined. Additionally included are defensive tactics like intrusion detection systems, frequent patching, robust authentication, and user education. This study intends to increase awareness and readiness against system-level threats in contemporary cyber security environments by looking at both offensive and defensive viewpoints.

IndexTerms **- System hacking, password cracking, privilege escalation, keylogging, backdoors, cybersecurity, intrusion detection, system vulnerabilities, ethical hacking, network security**

I. INTRODUCTION

One of our most revolutionary and rapidly expanding technologies has been the internet. Numerous benefits, such as email, electronic commerce, and instant access to a wealth of reference materials, have been brought about by the Internet's explosive growth. The number of computers connected to the internet is increasing, and wireless networks and gadgets are growing significantly. Because of the web's advanced technology, the government, corporate sector, and hence the general public are afraid that a criminal hacker will compromise their data or private information. These hackers are known as "black hat" hackers, and they will take the company's data and send it over the public internet.

Therefore, in order to overcome these significant problems, a new class of hackers—known as ethical or white hat hackers—arose. The definition of hacking, ethical hackers, their job in any organization, the many stages of hacking, etc. are all covered in this paper. Therefore, in the context of computer security, these ethical hackers or tiger teams would employ the same methods and strategies as hackers, but in a way that is lawful and does not include causing harm to the target systems or stealing data.

II. ETHICAL HACKING

Hacking is the process of identifying security flaws in a network or computer system and using them to obtain personal or corporate data. It claims that someone else's computer system was accessed without authorization. Hacking is the misuse of gadgets such as computers, smartphones, tablets, and networks to damage or corrupt systems, steal data, or interfere with data-related operations. In the current digital era, ethical hacking is crucial for protecting networks, systems, and data from malevolent attacks. With the increasing sophistication of cyber threats, companies want experts who can find and address security flaws before hackers take advantage of them. White-hat, or ethical, hackers employ the same tools and methods as malevolent hackers, but they do so with authorization and for defensive reasons. Their efforts aid in preventing financial losses, reputational harm, and data breaches. Ethical hacking is essential to preserving safety, privacy, and trust in the digital world because it actively tests and fortifies security measures. The figure 2.1 shows a hacker at a laptop, symbolizing cybercrime threats like identity theft, password breaches, bank fraud, and online spying.

Fig: 2.1 Ethical Hacker

Advantages of Hacking:
The following are some circumstances in which hacking is advantageous:

- To restore deleted data, especially if you can't remember your password.
- To strengthen network and computer security, penetration testing should be used.
- To implement enough preventive measures to stop security breaches.
- To have a computer system that prevents access from malevolent hackers.

Disadvantages of Hacking :
Hacking may be harmful if done with the intention of causing harm.

- It has the potential to cause a huge security breach.
- Unauthorized system access to confidential or sensitive data.
- The destruction of privacy.
- Fettering system functionality.
- Attacks that cause denial of service.
- A malicious attack on the network or system.

III. PHASES OF ETHICAL HACKING

The figure 3.1 illustrates the five key phases of ethical hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Clearing Tracks. These steps help ethical hackers identify and fix security vulnerabilities in systems.

Fig: 3.1 Ethical Hacker Steps

Reconnaissance: The collection of methods and techniques used to covertly get knowledge about the target systems is known as reconnaissance. Using the seven steps listed below, the ethical hacker aims to learn as much as they can about the target systems. Identifying the machines that are in use gathering preliminary data and identifying each port's services Network mapping, access point and port identification, and OS fingerprinting.

Scanning: Scanning constitute the second phase of penetration testing and ethical hacking. The most popular method used by pen testers to locate the open door is scanning. The purpose of scanning is to identify any vulnerabilities in the services that run on the port. During this stage, they must identify the operating systems, live host, firewalls, services, intrusion detection, perimeter equipment, routing, and general network topology (physical network layout) that are a part of the target company.

Gaining Access: The hackers then try to obtain access using a few tools and techniques after the observation is complete and every vulnerability has been tested. This basically focuses on getting the password back. Hackers can utilize either bypass methods or password cracking techniques for this.

Maintaining Access: After gaining access to the targeted systems, the hacker has two options: either keep a low profile and keep abusing the systems without the real user noticing, or take use of the systems and their resources and use them as a launchpad for testing and damaging other systems. The organization that causes a disaster will be destroyed by those two actions. Trojan horses enter at the program level, whereas rootkits enter at the operating system level. Attackers can transfer user names, passwords, and

credit card information on the system by using Trojan horses. Businesses that are able to identify the invaders by using intrusion detection or honeypot techniques.

Clearing Tracks: An criminal will remove proof of his existence and activity for a number of reasons, including evading detection and further punishing for trespass. For every invader who wants to stay anonymous and avoid detection, removing evidence—often referred to as "clearing tracks" is necessary. Typically, this process starts with On the victim system, remove any erroneous login credentials or any potential error messages produced by the attack procedure.
A buffer overflow attack, for instance, typically leaves a notification in the system logs that needs to be cleared. Making adjustments to avoid logging in to possible logins is the next area of concentration. Reviewing all system log files is the first step a systems administrator takes to identify unusual behavior on the system. Trespassers must utilize the tool to alter system logs in order for the administrator to be unable to follow them. Attackers want to make the system appear as it was before they gained access and created a backdoor for their own purposes.

IV.TOOLS USED IN ETHICAL HACKING:

The fundamental instruments used in a controlled laboratory setting to carry out the system exploitation process. Through the facilitation of reconnaissance, exploitation, and post-exploitation phases of the attack, these technologies provide a practical comprehension of adversarial tactics and defensive weaknesses.

1. Kali Linux: The attacker's computer was running Kali Linux, a Linux distribution based on Debian. Numerous tools for security auditing and penetration testing are included. The main platform for initiating attacks, conducting scans, and overseeing post-exploitation operations is Kali. It is perfect for simulating actual cyberattacks in a secure lab environment because of its interaction with the Metasploit Framework.

Features:

- A Linux operating system based on Debian that is intended for penetration testing.
- More than 600 cybersecurity technologies are pre-installed.
- Provides built-in support for ethical hacking frameworks like as Wireshark, Nmap, and Metasploit.
- Lightweight and virtual environment-optimized.

The attacker's computer was Kali Linux, which was operating in a virtual environment. It was employed for:

- When doing reconnaissance, start Nmap scans.
- To exploit the target, launch the Metasploit console (msfconsole).
- For post-exploitation activities like as data extraction, screenshot taking, and command execution, manage the Meterpreter shell.

2. Windows 7 (Target System): An unpatched virtual machine running Windows 7 Professional served as the study's target computer. Windows 7 is a high-value target since it is still present in many legacy systems even though it is out-of-date and unsupported. Its well-known flaws, such as the notorious MS17-010 (EternalBlue), offered a useful platform for evaluating the efficacy of exploits.

Features:

- widely used legacy OS that Microsoft no longer supports.
- susceptible to many known exploits, including MS17-010.
- It is perfect for exploitation testing because it lacks many contemporary security measures.

The target system was configured to be the Windows 7 computer. Important actions included:

- Turning off the firewall to mimic inadequate security practices.
- Use ipconfig to determine the machine's IP address.
- Maintaining the system's vulnerability to the EternalBlue exploit by leaving it unpatched.

3. Metasploit Framework: One popular and potent open-source exploitation framework is Metasploit. Ethical hackers can use it to test vulnerabilities, initiate exploits, send payloads, and carry out post-exploitation tasks. The SMB vulnerability in Windows 7 was exploited in this project using the ms17_010_eternalblue module, which produced a reverse Meterpreter shell.

Features:

- Foundation for creating, evaluating, and running exploits that is open source.
- Consists of modules for payloads, post-exploitation, scanners, exploits, and ancillary tools.
- Offers msfconsole, an interactive console for controlling attack sessions.

The functions carried out by Metasploit:

- started using msfconsole.
- Search ms17-010 and use 0 were used to choose the ms17_010_eternalblue exploit.
- The exploit command was used to launch the exploit after setting the target IP (RHOSTS).
- After successful exploitation, further system control was made possible by opening a reverse Meterpreter shell.

4. Meterpreter: Meterpreter is a sophisticated payload that runs in the Metasploit framework. Meterpreter offers an interactive shell that, after a system has been compromised, enables attackers to carry out commands, navigate the file system, capture screenshots, record keystrokes, and sustain access indefinitely—all without writing data to disk, which makes detection more difficult.

Features:

- Metasploit payloads are used to deploy a potent post-exploitation tool.
- Allows for in-memory operation (to escape antivirus detection).
- Allows for persistence, file sharing, screen capture, and process interaction.

Once the Windows 7 system was exploited, the Meterpreter shell allowed for:

- Directory traversal with cd and file enumeration with ls.
- Using download to obtain sensitive folders.
- use the snapshot command to take screenshots.
- Screenshare allows for real-time screen surveillance.

5. Nmap: A reconnaissance tool called Nmap (Network Mapper) is used for security audits and network discovery. It was used in this project to determine the operating system version, find open ports (such SMB port 445), and scan the target system. For OS identification, service version detection, and covert SYN scans, the command nmap -sS -sV -O was utilized.

Features:

- An open-source tool for security auditing and network discovery.
- Detects operating systems, service versions, open ports, and active hosts.
- Supports a variety of scan methods, including aggressive scans, OS detection, and SYN.

Nmap was used in two key stages:

- To detect active systems, use nmap -sn 192.168.0.1-255 for host discovery.
- For OS detection and target scanning, run sudo nmap -sS -O -T5 192.168.0.55 to find:

  Ports like 445 (SMB) are open.

  OS fingerprinting (found in Windows 7)

  Potential weaknesses (MS17-010)

6. Virtualization Software: Both the attacker's (Kali Linux) and the target's (Windows 7) computers were housed in a separate virtual environment using VMware Workstation or Oracle VirtualBox. This guarantees that the testing faithfully mimics attack surfaces found in the real world without affecting production systems.

Features:

- Permits several operating systems to run on a same physical computer.
- Provides options for network configuration (NAT, host-only, etc.).
- Allows for safe experimentation by offering system isolation and snapshots.

The function carried out by the Virtualization Software:

- hosted the target (Windows 7) and attacker (Kali Linux) computers.
- set up in host-only network mode to replicate a remote setting.
- IP-based communication between virtual systems was made possible to simulate realistic attacks.

V.TYPES OF CYBER HACKER:

Hackers are experts in computer networks and systems who gain access to systems by using their technical expertise. Hackers can be roughly divided into the following categories based on their goals and legality:

1. White Hat Hackers: Professional hackers with knowledge of cybersecurity are known as "white hat" hackers. They have the certification or authorization to hack the systems. By breaking into the system, these White Hat Hackers operate for governments or groups. They take advantage of the organization's cybersecurity flaws to hack the system. The purpose of this hack is to evaluate the organization's cybersecurity posture. By doing this, they find their weaknesses and address them to prevent outside attacks. White hat hackers operate in accordance with the laws and guidelines established by the government. Ethical hackers are another name for white hat hackers.

Motives & Objectives: These hackers' objectives are to assist companies and to find security flaws in networks. They seek to defend and support businesses in their continuous fight against cyberthreats. Any person who assists in preventing cybercrimes against the company is known as a "white hat" hacker. They assist businesses in establishing defenses, identifying weaknesses, and resolving them before other cybercriminals do.

2. Black Hat Hackers: The black hat Hackers are skilled computer specialists as well, but they act maliciously. In order to gain access to systems where they are not authorized, they attack other systems. Once they have access, they might either destroy the system or steal the data. These hackers' methods vary according to their level of expertise and ability to hack. Because the hacker is a criminal due to their aims. It is impossible to determine the scope of the hacking breach or the malevolent action intent of the individual.
Motives & Objectives: to break into a company's network and take money, bank information, or private data. Typically, they harass their target company, sell the resources on the illegal market, or use them for personal gain.

3. Script Kiddies: Half-knowledge is always perilous, as is well known. In the realm of hacking, the Script Kiddies are amateur hackers. Using scripts written by other hackers, they attempt to breach the system. They attempt to breach websites, networks, or systems. The sole goal of the hacker is to attract their peers' attention. Children that lack a thorough understanding of the hacking process are known as "Script Kiddies."
Motives & Objectives: DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks are common Kiddie Script attacks. This merely indicates that an IP address collapses due to an overwhelming amount of excessive traffic. For example, have a look at a few Black Friday purchasing websites. It makes things confusing and stops other people from using the service.

4. Green Hat Hackers: Hackers who become proficient in hacking are known as "green hat" hackers. Because of their purpose, they differ slightly from the Script Kids. The goal is to work toward and acquire the skills necessary to become a proficient hacker. They are searching for chances to pick the brains of seasoned hackers.

5. Red Hat Hackers: Eagle-Eyed Hackers and Red Hat Hackers are interchangeable terms. These hackers resemble white hackers in certain ways. The goal of the red hat hackers is to thwart the black hat hackers' onslaught. Red hat and white hat hackers vary in that they both use the same method of hacking with malicious intent. When it comes to combating malware or black hat hackers, red hat hackers are extremely brutal. The entire system configuration may need to be replaced as a result of the red hat hackers' ongoing attacks. The five categories of hackers mentioned above are commonly used in the field of cybersecurity.

VI.CONCLUSION:

As long as system developers continue to use antiquated architectures that were not initially created with security in mind, cybersecurity issues will exist. Patching these susceptible systems with ad hoc methods frequently yields short-term rather than long-term cures. Intrusion testing teams' efforts alone cannot guarantee security because their results could give false hope. Rather, businesses need to take a holistic approach that incorporates security into all tiers of their IT architecture. This involves diligent system management procedures, proactive intrusion detection, ongoing system monitoring, and effective staff awareness campaigns. Each of these components is essential to creating a strong security posture. Devastating outcomes like cyberattacks, data breaches, monetary losses, or damage to one's reputation might result from a single technological or human error. As a result, in today's linked world, maintaining security is not only a technical necessity but also a crucial organizational goal.

VII. REFERENCES

[1] G. R. Lucas, “Cyber warfare,” in The Ashgate Research Companion to Military Ethics, 2016.
[2] P. Engebretson, “Reconnaissance,” in The Basics of Hacking and Penetration Testing, 2011.
[3] Ehacking, “Scanning and Enumeration- Second Step of Ethical Hacking,” ehacking, 2011.
[4] R. Baloch, Ethical Hacking and Penetration Testing Guide. 2017. [1] “Is Ethical Hacking Ethical?,” Int. J. Eng. Sci. Technol., 2011.
[5] S.-P. Oriyano, “Introduction to Ethical Hacking,” in CEHTMv9, 2017.
[6] B. Sahare, A. Naik, and S. Khandey, “Study of Ethical Hacking,” Int. J. Comput. Sci. Trends Technol., 2014.
[7] S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, “Ethical hacking: The need for cyber security,” in IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017, 2018, doi: 10.1109/ICPCSI.2017.8391982.
[8] G. R. Lucas, “Cyber warfare,” in The Ashgate Research Companion to Military Ethics, 2016.
[9] P. Engebretson, “Reconnaissance,” in The Basics of Hacking and Penetration Testing, 2011.
[10] Ehacking, “Scanning and Enumeration- Second Step of Ethical Hacking,” ehacking, 2011.
[11] R. Baloch, Ethical Hacking and Penetration Testing Guide. 2017.
[12] Norton, “What is the Difference Between Black, White and Grey Hat Hackers?” Emerging Threats, 2019.
[13] S. Tulasi Prasad, “Ethical Hacking and Types of Hackers,” Int. J. Emerg. Technol. Comput. Sci. Electron., 2014.[14] A. Boudreau, L. J. Van’t Veer, and M. J. Bissell, “An ‘elite hacker’: Beast tumors exploit the normal microenvironment program to instruct their progression and biological diversity,” Cell Adhesion and Migration. 2012, doi: 10.4161/cam.20880.